Integrating Security into Large System Acquisitions

NIAP

GAO

MITRE

FAA

Agenda

- Welcome
- About the NIAP
- Introduction
  - Some context for today's topic
  - Agenda for the rest of the day

NIAP Goal

- The long-term goal of NIAP is to offer services and methods to increase the level of trust consumers have in their systems and networks
  - products
  - systems
  - people
  - processes

Security Requirement Specification

- Evolution of Common Criteria (CC)
- Security Requirement Forums
  - Healthcare
  - Insurance
  - Audit
  - Smart Card
- Cryptographic Module (FIPS 140)

Testing and Evaluation

- CC Evaluation and Validation Scheme
- Uses Common Criteria
  - Security Targets
  - Protection Profiles

Information Assurance Research/Development

- CC Toolbox
- Certification/Accreditation
- IA In Acquisition

Today's Topic: Security in the Acquisition Process

- **The Perceived Problem**

  Security Community and Acquisition Community are different communities, each with their own processes and languages

- **Result**

  Acquired systems where security properties of the system have not been considered as an integral part of the acquisition process resulting in risky implementations

Security in the Acquisition Process (cont)

- **A Proposed Solution**

  A method to integrate security engineering principles into the acquisition process in a manner that allows stake holders to make intelligent risk management decisions not only during the course of the acquisition cycle but as part of the full development life cycle

The rest of the day…..

- 10:00-10:45

  The Proposal – Ms. Deb Bodeau, MITRE

- 11:00-11:30

  The Proposal in the Context of :

  - System Engineering Acquisition Policy and Standards – Rob Simmons, MITRE
  - Certification/Accreditation – Dr. Ron Ross, NIAP

The rest of the day (cont)…

- 11:30-12:15
  - Experience thus far in application

    The FAA Experience: Dr. Marshall Abrams, MITRE and Mr. Joe Veoni, MITRE
- 1:30-3:15
  - Break Out Sessions

    - Objective: Get your ideas and feedback

Last Slide

Feedback/Discussion: Breakout Sessions – 1:30-3:15

- Composition/Decomposition – Rm: A

  Facilitator: Deb Bodeau

- Specification and Process – Rm: D

  Facilitator: Kris Britton

- Procurement Alternatives – Rm: C

  Facilitator: Marshall Abrams

- Certification/Accreditation – Rm: Green

  Facilitator: Arnold Johnson

Last Slide

Next Steps

- Solicit “Pilot Applications” of the Methodology

Next Steps (cont)

- NIAP Steering Group Establishment
  - Charter
    - Consider your feedback
      - Send comments/questions to: isa_steer@nist.gov
    - Aid “pilot applications” in the use of the methodology
    - Create Federal Guidance on incorporating security into the acquisition process

Last Slide

Specifications Process In Large Systems

- Should the System PP's be Verified / Validated?
  - Yes, but not NIAP -
- What Role do NIAP PP's play in the system PP?
  - Developers want product evaluation – once – applies against all PP's
- How do we ensure that the proposal address the system PP?
  - Include evaluation criteria
- How do we evaluate contractor evidence that a system meets PP requirements?
  - OT&E, Field trials, double-edge-sword

COMMENTS:

- Evaluate products they play a role in the SSP
- Requirements engineering – lags the SPP
- How much of the FAA SPP can be applied against other organizations (e.g. DoD)
- Tie validated products to proposal – currently don’t
- The ssp supports the integrator, plays less of a role wrt product developer
- Granularity – single NAS SSP or subsets. One SSP drives to highest common denominator (expensive)

Continued

- SSPT should be released with the enterprise architecture
- Take elemental PP and use them to design SSP's
- Merge Security Admin CONNOP with the SSP – early
- SSP's are beneficial – but must have a way to modify it easily because requirements change.
- 'Vulnerabilities shall not be introduced into the system'; the process to detect vulnerabilities must be specified (e.g. detailed architecture)
- System engineer must participate in requirements writing